UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,529	12/31/2003	Kevin R. Driscoll	H0005071	5548

128 7590 09/10/2009
HONEYWELL INTERNATIONAL INC.
PATENT SERVICES
101 COLUMBIA ROAD
P O BOX 2245
MORRISTOWN, NJ 07962-2245

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2436	
MAIL DATE	**DELIVERY MODE**
09/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/750,529
Filing Date: December 31, 2003
Appellant(s): DRISCOLL, KEVIN R.

Gregg A Peacock
Reg.No. 45,001
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 04/27/2009 appealing from the Office action mailed 02/26/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final action

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US Pub No 2002/0080974	Grawrock.	12-27-2000
WO 00/18162	Johnson, P.K. et al.	04-03-2000

Public key encryption and digital signature: How do they work? Entire Contents 2004 by CGI Group Inc.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. Claims 1-8, 13-31are rejected under 35 U.S.C. 102(e) as being anticipated by Grawrock et al (herein after referred to as Grawrock) US Patent NO 2002/0080974 B2.

2. As per claim 1,13,24: Grawreock discloses a method/apparatus/a physical machine-readable medium comprising: receiving an ephemeral value from a challenging device (See 0029 and Fig 3 step 320(i.e., transmit ephemeral credential); retrieving data whose content is known to the challenging device (See 0017 and Fig 3 step 320(i.e., identity credential to the requestor));performing data authentication, wherein performing the data authentication (See Fig 3 steps 325,330(i.e., validate identity using identity credential))comprises generating a digital signature of the data based on the ephemeral value (See 0028-0029,0034 and see Fig 3 steps 310,315(i.e., produce ephemeral credential)); a cryptographic key having a value that is equal to the ephemeral value(See0033- 0034 and Fig 4 steps 410,420(i.e., ephemeral asymmetric public key matches EAPUK); and transmitting the digital signature to the challenging device (See 0034 and Fig 3 step 320(i.e., transmit ephemeral credential).

3. As per claim 2, 25: Grawreock discloses the method wherein receiving the ephemeral value from the challenging device comprises receiving a randomly generated number from the challenging device (See 0028, 0030).

4. As per claim 3, 26: Grawreock discloses the method wherein retrieving the data comprises retrieving at least part of application code (See 0017).

5. As per claim 4,27: Grawreock discloses the method wherein generating the digital signature of the data based on the ephemeral value comprises generating a one-way hash across the data with the cryptographic key having a value that is equal to the ephemeral value (See 0033-0034).

6. As per claim 5,28: Grawreock discloses a method comprising: receiving, into a response device, an ephemeral value from a challenge device (See 0029 and Fig 3 step 320); retrieving data from an address space in the response device, wherein the data is known to the challenge device and the response device (See 0017 and Fig 3 step 320);performing data authentication of data stored in the challenge device(See Fig 3 steps 325,330 and 0015,0017), wherein performing the data authentication comprises generating a hash across the data using the ephemeral value as a key of the hash (See 0028-0029,0034 and Fig 5 steps 510,520); and transmitting at least part of the hash to the challenge device(See 0034 and Fig 5 steps 500,510).

7. As per claim 6,29: Grawreock discloses the method further comprising generating a reduced hash based on the hash, wherein transmitting the ephemeral value and the at least part of the hash to the challenge device comprises transmitting the ephemeral value and the reduced hash to the challenge device (See 0033-0034).

8. As per claim 7, 30: Grawreock discloses the method wherein retrieving the data from the address space in the response device comprises retrieving application code to be executed in the response device (See 0014, 0017).

9. As per claim 8, 31: Grawreock discloses the method wherein retrieving the data from the address space in the response device comprises retrieving configuration parameters of the response device (See Fig 3 step 320).

10. As per claim 10: Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating an application executable (See 0017, 0021).

11. As per claim 11: Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating at least one security parameter (See Fig 3 step 320).

12. As per claim 12: Grawreock disclose the method wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature (See Grawreok 0033-0034 and Fig 4 steps 410,420).

13. As per claim 14: the combination of Johnson and Grawreock disclose the apparatus wherein the I/O logic is to receive the request for authentication from a challenge device, the I/O logic to transmit the cryptographic hash back to the challenge device (See Grawreock Fig 2 and 0033-0034).

14. As per claim 15: the combination of Johnson and Grawreock disclose the apparatus wherein the storage medium is a nonvolatile memory (See 0021-0022, 0024).

15. As per claim 16: the combination of Johnson and Imai disclose further comprising a data selection logic to select less than all of the data, wherein the at least part of the data is the less than all of the data (See 0024,0028).

16. As per claim 17: the combination of Johnson disclose the apparatus wherein the data selection logic is to select less than all of the data based on a random number based selection of segments of the data (See 0028,0030-0031).

17. As per claim 18: Grawreock the apparatus wherein the data comprises an application to be executed in the apparatus (See 0017, 0021).

18. As per claim 19: Grawreock discloses the apparatus wherein the data comprises at least one security parameter of the apparatus (See Fig 3 step 320).

19. As per claim 20: Grawreock discloses a challenge device to authenticate data presumably stored in a response device, the challenge device comprising: a storage medium to store a copy of the data presumed to be stored in the response device (See (See 0028,0030); a key generation logic to generate an ephemeral value (See 0025); an input/output (I/O) logic to output a request for authentication to a response device, wherein the request includes the ephemeral value, the I/O logic to receive a first digital signature from the response device in response to the request for authentication(See Fig 2 step 200 and 0029-0030); a signature logic to retrieve the copy of the data and the ephemeral value and to generate a second digital signature(See 0029-0030); and an authentication logic to compare the first digital signature to the second digital signature, wherein the data is authenticated if the first digital signature equals the second digital signature(See 0030 and Fig 5 steps 530,540).

20. As per claim 21: Grawreock discloses the challenge device wherein the ephemeral value comprises a randomly generated value (See 0028, 0030).

21. As per claim 22: Grawreock discloses the challenge device wherein the data comprises application code to be executed by the response device (See 0014, 0017).

22. As per claim 23: Grawreock discloses the challenge device wherein the data comprises at least one configuration parameter of the remote device (See Fig 3 steps 320).

Claim Rejections - 35 USC § 103

23. Claims 9-12,32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson, P. K., et al(hereinafter referred as Johnson) (W0 00/18162) in view of Grawrock et al (herein after referred to as Grawrock) US Patent NO 2002/0080974 B2 .

24. As per claim 9,32: Johnson discloses a method comprising: authenticating data having predictable content and stored in an address space of a remote device, the authenticating comprising: generating a random number (See col. 10 lines 20-33); transmitting the random number to a remote device presumably having the data (See col. 6 lines 17-24 and Figs 2,3); receiving, from the remote device, a first digital signature that is representative of the data (See col. 6 lines 25-33 and abstract);

Johnson does not explicitly teach generating a second digital signature with a cryptographic key having a value that is equal to based on the random number; and comparing the first digital signature to the second digital signature.

However Grawrock teaches generating a second digital signature with a cryptographic key having a value that is equal to based on the random number(See 0028-0029,0034 and see Fig 3 steps 310,315) and comparing the first digital signature to the second digital signature(See 0033-0034& Fig 5 steps 530,540).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to modify the teaching method of Grawrock within Johnson method in order to enhancing the security of the system.

25. As per claim 10, 33: the combination of Johnson and Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating an application executable (See Johnson col. 7 lines 1-3).

26. As per claim 11,34: the combination of Johnson and Grawreock disclose the method wherein authenticating the data having predictable content comprises authenticating at least one security parameter (See Johnson col. 7 lines 1-3).

27. As per claim 12, 35: the combination of Johnson and Grawreock disclose the method wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature (See Grawreok 0033-0034).

(10) Response to Argument

With respect to claims 1-8 and 13-31, Appellant argued that Grawrock fails to teach performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value. Appellant argued that none of Examiner's cited portions in Grawrock teach such generating a digital signature using a key that has a value equal to an ephemeral value.

Examiner would point out that Grawrock teaches generating a digital signature of the data based on the ephemeral value (See Grawrok 0028-0029, 0034 and see Fig 3 steps 310,315(i.e., produce ephemeral credential)). It is understood by the examiner, that digital signature implies: encryption of a message with a private key (i.e., signing the message) and decrypting of the message with a public key (i.e., verification of the message) *[See, "Public Key Encryption and Digital Signature: How do they work?" provided with this action as an evidence, sections 1.2 and 1.3]* and therefore, the use of ephemeral keys as cryptographic keys in Grawrock is understood by the examiner to be equivalent to that of digital signature using a key [See Grawrock, 0035-0036].

Appellant argued that Grawrock does not disclose performing data authentication. Appellant further argued that the office alleges that performing encryption is equivalent to generating a digital signature or hash. There is no disclosure of any advantage that performing data authentication.

Examiner would point out that Grawrock teaches performing data authentication (See Fig 3 steps 325,330 (validate identify using identify credential).The examiner also want to point out that it's well known in the art that using authentication and encryption to protect data. The examiner further points out that, the system in Grawrok relates to use of ephemeral value as a cryptographic key to perform encryption/decryption of data.

For example Digital signature is a mechanism by which a message is authenticated & public key is the only key that can decrypt that message, a successful decryption constitutes a digital signature verification (See section 1.3) (i.e., the using ephemeral value as a cryptographic key to perform encryption is equivalent to use of an ephemeral value as a cryptographic key generate a digital signature).

Appellant argued that the combination of Johnson and Grawrock do not teach generating a second digital signature with a cryptographic key having a value that is equal to the random number.

Examiner would point out that the combination of Johnson and Grawrock teach generating a second digital signature with a cryptographic key having a value that is equal to the random number. (See Grawrock 0033-0034& Fig 5 steps 530,540)

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Fikremariam Yalew/

Conferees:

Beemnet Dada

/Beemnet W Dada/

Primary Examiner, Art Unit 2435

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436